

REMARKS

Claims 29, 32, 36 and 38-43, as amended, remain herein. Claims 31 and 35 are canceled without prejudice. The subject matter of former claim 31 has been added to claim 29, and the subject matter of former claim 35 has been added to claim 41.

Applicants and their undersigned attorney appreciate the courtesies extended by SPE Fischer during the telephone interview on January 24, 2011, which was the culmination of partial conversations initiated by calls by applicants' undersigned attorney to Examiner West on January 6 and 11, 2011. The arguments made by applicants' attorney during the January 24 interview are stated in the remarks below.

1. Claims 35 and 41-43 were rejected under § 103(a) over Waters '589 in view of O'Boyle '329.

As stated above, claim 41 has been amended to include the subject matter of former claim 35.

The Office Action alleges that Waters discloses, inter alia:
a content reproducing device reading from an optical disk a cipher key and identification information unique to the optical disk; (citing Waters, col. 4, lines 32-67 and col. 5, lines 34-67);
such content reproducing device encoding specific data using the cipher key (citing Waters, col. 6, lines 35-67).

However, contrary to the indications in the Office Action, the Waters disclosure does not include any specific “cipher key” that corresponds to the “cipher key” recited in applicants’ claims. And, Waters does not disclose any encoding process that uses such a cipher key.

Waters initially creates an “identifying value” which is sequential and relates to a location of physical damage to tracks and/or sectors of a CD-ROM. See generally, Waters, col. 3, line 10 through col. 4, line 67. Waters encrypts the identifying value (or a composite value created by combining an identifying value with another unique value). The encrypted value is then marked on the hub of the disk (see Waters, Figs. 4A and 5A, and col. 3, line 30 through col. 4, line 58).

However, the encryption mentioned by Waters is not stated or demonstrated to use any specific “cipher key” to enable encryption of an identifying or composite value. Waters simply encrypts numbers. How this is done is not disclosed by Waters.

Applicants’ claimed invention is distinct from anything disclosed or suggested by Waters because a specifically defined cipher key is recorded in the form of stripe patterns of a reflective layer in a disk, which layer has been laser trimmed. Such a specific cipher key is used to enable encryption of specific data, such as accounting information.

The stripe patterns in the disks of applicants’ invention are extremely difficult to counterfeit, so that the security of disks embodying applicants’ claimed invention is much higher than those using a Waters system that does not include any specific cipher key or specific encryption method using such a cipher key. Further, contrary to the argument at page 6, point 9, of the Office Action, there is no disclosure in Waters, col. 6, lines 1-34 of readable information

encoded in an area overlapping a pre-pit region of an optical disk, as recited in applicants' claim 29.

O'Boyle '329 likewise does not disclose or suggest applicants' claimed invention. The prior Office Action (04/27/10) admits that O'Boyle '329 fails to disclose any "stripe pattern extending in the radial direction." Further, O'Boyle '329 does not disclose that among identification information and a cipher key, which are recorded in the stripe patterns of an optical disk, a cipher key is used to encode data to be communicated to a server, and identification information is transmitted to a server and used to select a decode key on the server.

According to O'Boyle '329, a cipher key used to encrypt encoded accountable data is not recorded in the card, whereas applicants' claimed cipher key is recorded in the optical disk.

Further, O'Boyle '329 requires that the validity of the card be determined by directly comparing (i) encoded data read from the card, and (ii) the data previously encoded and stored. Therefore, the O'Boyle '329 system is different from applicants' invention wherein identification information is transmitted to the server and used to select the decode key on the server. In applicants' invention, the disk containing the data is determined to be valid when both the identification information and cipher key are valid after selecting, on the server, a decode key based on identification information.

Thus neither Waters nor O'Boyle, alone or combined, could achieve preventing decoding of encoded data from any unauthorized optical disk, even having either one of the valid identification information or cipher key. Further, neither Waters nor O'Boyle, alone or in

combination, would have suggested that it is unnecessary to encode all the data possibly communicated and store all of that encoded data, in advance, on the server.

Neither Waters nor O'Boyle discloses all elements of applicants' claimed invention. Nor is there any disclosure, teaching, or suggestion in either of Waters or O'Boyle that would have suggested the desirability of combining or modifying any portions thereof to render obvious applicants' claimed invention. Reconsideration and withdrawal of this rejection are respectfully requested.

2. Claims 29, 31 and 32 were rejected under 35 USC § 112, paragraph two. The Office Action also stated that five elements of those claims invoke §112, paragraph six. The Office Action further stated that "the written description fails to clearly link or associate the disclosed structure, material, or acts to the claimed function such that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function." (Office Action, 10/28/2010, p. 2). The Office Action further stated that applicants are "required" to either (a) amend the claims, (b) amend the written description, or (c) state "where the corresponding structure, material, or acts are set forth in the written description of the specification that perform the claimed function."

Applicants note that this rejection under § 112, paragraph two, was not stated in either of the two previous Office Actions (August 4, 2009 and April 27, 2010). Such a possible issue was raised for the first time by SPE Fischer at the outset of the interview conducted at the PTO on July 20, 2010—to the surprise of applicants' undersigned attorney and to applicants. Even

though no such rejection had been stated on the record, in a good faith effort to advance the prosecution of this application, applicants identified at pages 8-9, and attached exhibits, of the Amendment filed August 23, 2010, specific parts of their disclosure which support the claimed reading means, encoding means, and communicating means recited in claim 29 (and dependent claims 32 and 38).

Because the Office Action mailed October 28, 2010 made no mention whatsoever of the aforementioned showing which applicants had made in the Amendment filed August 23, 2010, applicants requested their undersigned attorney to request the PTO to specify what, if any, aspects of that showing were allegedly inadequate. And it was for that specific purpose that numerous calls were made to Examiner West, which culminated in the January 24, 2011 telephone conversation initiated by SPE Fischer. No really specific answer to applicants' inquiries was received during the January 24, 2011 conversation, wherein SPE Fischer primarily relied upon the conclusory statement at the bottom of page 2 of the Office Action (quoted above, herein).

Accordingly, applicants herebelow again present the facts stated in and with the prior Amendment, here related to the five claim elements mentioned in the latest Office Action:

- (1) Claim 29, "reading means for reading a cipher key . . ."
- (4) Claim 31, "reading means for reproducing . . ."
- (5) Claim 32, "reading means for reading the certain information . . ."

See, for example, applicants' FIGS. 6A and 6B, annotated copies of which are attached hereto as Exhibit 6A/B and Exhibit 3 which are annotated copies of pages of applicants'

specification. These exhibits were also attached to the Amendment filed herein August 23, 2010. As illustrated in Figs. 6A/6B, in first computer 909 there is BCA reproducing part 820, which is the “reading means.” In applicants’ specification, page 8, lines 28-32, there is disclosure of the structure of the reading means.

(2) Claim 29, “enclosing means for encoding . . . “

In first computer 909, second cipher encoder 831 encodes accounting data 830, and thus is the “encoding means.” At page 10, lines 29-35, there is disclosure of the structure of the encoding means.

(3) Claim 29, “communicating means for communicating . . . “

In first computer 909, communication part 822 is the “communicating means.” In addition, there is a second cipher decoder 832 that decodes enciphered accounting information in the third computer 828, which corresponds to a “server” in applicants’ claim 29. At page 11, lines 1-10, there is disclosure of the structure of the communicating means. See pages 8-11 of applicants’ specification, copies of which are attached thereto as Exhibit 3.

It continues to be applicants’ belief that the above-identified portions of applicants’ disclosure adequately link and associate the disclosed structures and materials to the claimed functions so that one of ordinary skill in the relevant art would recognize what disclosed structures or materials perform the claimed functions – thereby satisfying § 112, paragraph two.

For all of the foregoing reasons, reconsideration and withdrawal of the rejection are respectfully requested.

3. Claims 29, 31, 32 and 38 were rejected under 35 USC § 103(a) over Waters in view of O'Boyle, further in view of Tanabe '767.

Claim 29 is amended to include the subject matter of former claim 31.

The device claimed in claims 29, 32 and 38 includes elements that correspond to elements of claim 41 that are missing from the prior art. The distinctions pointed out above herein between applicants' claims and the disclosures of Waters and O'Boyle, are similarly relevant to claims 29, 32 and 38.

Tanabe '767 does not disclose the stripe patterns of applicants' claimed invention. The stripe patterns of Tanabe are made by etching, which is not unique to each disk and is easy to counterfeit. In contrast, the stripe patterns of applicants' invention are made by laser trimming a reflective layer in each disk, which results in a unique stripe pattern for each disk. Applicants' laser trimmed stripe patterns are therefore very difficult to counterfeit. And, the identification information and cipher key are recorded in such stripe patterns, and the encryption of specific data using such identification information achieves a higher security level.

Further, contrary to the indication in the Office Action at page 4, lines 1-2, there is no disclosure in those cited portions of Waters that indicates that the Waters disk includes a reflective layer that has been trimmed with a laser beam, let alone the stripe patterns of applicants' claimed invention. The Office Action overreaches the objective disclosures of the references in an effort improperly to find applicants' invention therein.

There is no disclosure or teaching in any of Waters, O'Boyle or Tanabe, of all elements of applicants' claimed invention. Nor is there any disclosure or teaching in any of those references or anything else in this record that would have suggested modifying or combining same effectively to anticipate or suggest applicants' presently claimed invention. Thus, there is no disclosure or teaching in any of the cited references that would have suggested applicants' claimed invention to one of ordinary skill in this art. Reconsideration and withdrawal of the rejection are respectfully requested.

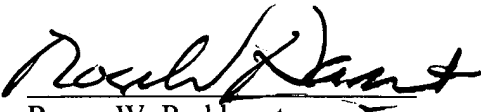
* * * * *

For all the foregoing reasons, all claims 29, 32, 36 and 38-43 are now proper in form and patentably distinguished over all grounds of rejection stated in the Office Action. Accordingly, allowance of all claims and a notice to that effect are respectfully requested. The PTO is hereby authorized to charge/credit any fee deficiencies or overpayments to Deposit Account No. 19-4293. If further amendments would place this application in even better condition for issue, the Examiner is invited to call applicants' undersigned attorney at the number listed below.

Date: January 27, 2011

STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795
Tel: (202) 429-3000
Fax: (202) 429-3902

Respectfully submitted,


Roger W. Parkhurst
Reg. No. 25,177

Attachments: Exhibits 3, and 6A/B

With reference to Fig. 6, the overall system of a cipher software unlatching system, narrowed down to the operations of password issue, cryptocommunication, and orderer certification, will be described. The steps in a press factory are nearly the same as in Fig. 1, so the original disk 800 and the completed disk 809 are not shown.

In a press factory 811, a cipher encoder 812 enciphers the data in the plaintexts 810 of the first to the '1- m'th contents or scrambles the picture signals therein with the first to '1- m'th cipher keys 813, respectively. The data or the signals are then recorded on an original optical disk 800. Disk-like substrates 809 are pressed from the original disk 800. After a reflecting film is formed on each substrate 809, the two disk-like substrates are laminated together. Thereafter a completed disk 809 is made. Recorded in the BCA areas 814 of completed disks 809 are different IDs 815 and/or first cipher keys 816 (public keys) and/or second cipher keys 817 (public keys) and second computer connection addresses 818 so as to make disks 801 each with a BCA. The disks 801 are distributed to users.

The contents of these disks have been enciphered. Therefore, in order to reproduce the contents of each of the disks, it is necessary to get a password from a password issue center, an electronic shop or a mall, by paying a charge. That procedure will be described next.

In a user's first computer 909, if a reproducer 819 reproduces a distributed disk 801 with a BCA, a BCA reproduction part 820 including a PE-RZ demodulation part reproduces the data of the ID 815, first cipher key 816, second cipher key 817 and/or connection address 818. In order to get a password, the connection address 818 of the second computer 821a, which is the server of a password issue center 821, is accessed through a

communication part 822 via the Internet or another network 823, and the ID is transmitted to the second computer 821a.

5 Here, the cryptocommunication procedure will be described. The second computer 821a receives the ID 815 from the user's reproducer 819. Then, the second computer or server 821a of the password issue center 821, which is called a 'mall' or an 'electronic shop' has a cipher key database 824. This database contains a table
10 of the secret keys which are the decoding keys corresponding to the disks' own IDs or the first cipher keys 816 of the IDs, that is the first decoding keys 825 and the IDs. The server can therefore search for the first decoding key 825 based on the received ID. Thus
15 cryptocommunication is completed from the first computer to the second computer 821a. In this case, if the first cipher key and first decoding key are common keys of a common key cipher, not of an public key cipher, they are the same key.

20 If the user wants to use part of the enciphered contents stored on the disk 801, which may be 1,000 in number, for example, the content number 826 of which is 'n', the user sends to the second computer 821a the cipher which is the content number 826, that is, 'n'
25 enciphered with the public key which is the first cipher key 816 by the first cipher encoder 827 composed of public key cipher functions. The second computer 821a searches for the first decoding key 825 for decoding this cipher as stated above. It is therefore possible
30 securely to convert this cipher into plaintext. Thus, the cipher protects the privacy of the user's order data.

In this case, a signature may be made by means of the secret key of the public key cipher as the first cipher key 816. This method is called 'digital
35 signature'. For a detailed explanation of the operation

of 'digital signature', see, for example, 'Digital Signature of E-Mail Security by Bruce Schneider 1995'.

Back to the cryptocommunication, the cipher is sent through the communication part 822 and network 823 to the first cipher decoder 827 of the password issue center 821. Thus the first cipher decoder 827 decodes the cipher by means of the first pair cipher key 825 pairing with the first cipher key 816.

In this case, because only the one disk has the public key, it is possible to reject invalid orders from third parties' disks. In other words, because each disk can be certified, it is possible to certify the user who owns the disk. It is thus certified that the content number 'n' represents a particular individual's order. It is therefore possible to exclude invalid orders of third parties.

If the public key 816 is secret, this method can technically be used to send a credit card number, or other accounting data which requires high security. Generally shops called 'malls' however, do not settle users' accounting data electronically, because there is no guarantee of security. Only the accounting centers 828 of credit card companies, banks and the like can deal with users' financial data. Presently, security standards such as secure electronic transaction (SET) are being unified, so it is probable that Rivest, Shamir and Adleman (RSA) 1024 bit public key ciphers will be used and the encipherment of financial data will be possible.

Next, the accounting data cryptocommunication procedure of the present invention will be shown. First, by using the second cipher key 817 of the public key cipher reproduced by the BCA reproduction part 820, the second cipher encoder 831 enciphers the accounting data 830 such as an individual's credit card number with a public key system cipher such as RSA. The enciphered

encode
encode

data is sent from the communication part 822 through the second computer 821 to the cipher decoder 832 of the third computer 828. In this case, if there is a need for digital signature, the secret key 829 is used as the second cipher key 817.

Similar to the procedure for the cipher key of the second computer 821a of the password issue center 821, it is possible to search the cipher key database 824a for the second decoding key 829 corresponding to the ID or the second cipher key 817. By using this decoding key 829, the second cipher decoder 832 can decode the enciphered accounting data.

If a digital signature is made by the second cipher encoder 831 with the secret key 829, the user's signature can be confirmed in the second cipher decoder 832. The accounting center 828 can thus get the user's credit card number, bank card number, bank password, or other accounting data safely even via the Internet. In open networks such as the Internet, security comes into question. By means of this system, however, it is possible to make cryptocommunication or certification without fault, because the cipher key (public key) for cryptocommunication or the secret key for digital signature has been recorded in the BCA. It is therefore possible to prevent third parties' unauthorized accounting and orders. In addition, because it is possible to use various public keys for different disks, that is, different users, the confidentiality of communication is improved, and the possibility of users' accounting data leaking to third parties is reduced.

Referring back to Fig. 6, the procedure for issuing a password and the procedure for unlatching with a password will be explained. The password issue center 821 includes a password generation part 834 with an operation expression of public key ciphers etc. Part 834